No Gods, No Servers

Decentralized Darknet Communication on Freenet

Michael Grube
@michaelgrube
github.com/mgrube

Fundamentals

Darknets

- Connections and participants are hidden
- Not easily accessible via the web(clearnet)
- Usually decentralized
- Examples:
    - I2P
    - Freenet
    - Tor

Freenet

- Created in 2000
- Peer to peer network - overlay network
- Distributed Data Store
- Designed to avoid state censorship
- Darknet capability introduced in 2007
- Completely Decentralized in Darknet Mode

Storage

- Keyspace distributed evenly across the network
- All nodes participate
- Opportunistic caching - BitTorrent effect with no tracker
- Data may be forgotten
- Insert data, Go Offline

Network Operation

Opennet:

- Trusted community seednodes are used to coordinate connections
- Semi-centralized
- Attacks more detectable by the community
- Risky
- Surveillance through correlation attacks

Network Operation

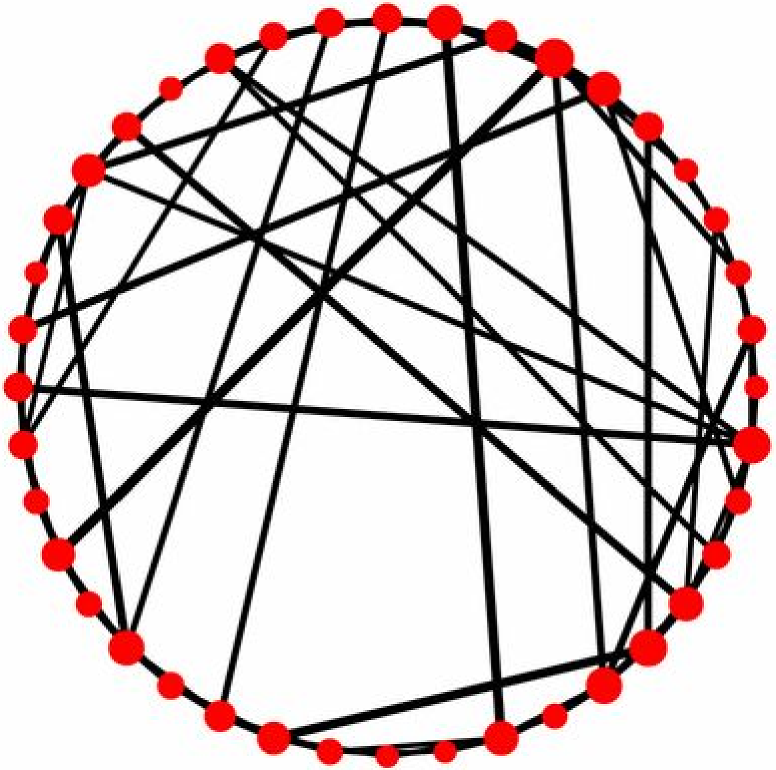
Darknet:

- Trusted peers are selected
- Efficient Routing
- Metadata is concealed
- Much safer than opennet
- Operates through a swapping mechanism

Mix: Have darknet peers while using opennet

Darknet Routing/Small World Networks

- “It’s a Small World!”
- Small World Routing
- Metropolis-Hastings Sampler for Small World Network distribution
- Connect to Friends, Talk to World
- No central point of failure
- DDoS nearly impossible



Diving In

Content Hash Keys

- The most basic form of storage on freenet
- Key corresponds to SHA256 hash of file
- Unchanging
- One piece of data
- Anyone may re-insert

Example:

CHK@XDPb43ZD6-yd9aNokAWdW76CDOYVzIlsjATS2xzJtKk,WXNLUIFBRAxs7Vq-eRxfrTJTPG0fFVgXolzUarhXEOM,AAMC--8/bman.jpg

Signed Subspace Key

- Public/Private Keypair Signed Space
- Content is added by a secret key that signs data
- May contain sets of files or data
- Anybody with private key may add data

Example:

SSK@fN3A5QeuvTLgR2KF8xmkNEIVTkBfmUQy2sCTCU1~hGk,vj3PbLWWB~dvDesZKjeyqHFnhxLDtbUKcq2N8xXYERg,AQACAAE/turtles.txt

SSK@fN3A5QeuvTLgR2KF8xmkNEIVTkBfmUQy2sCTCU1~hGk,vj3PbLWWB~dvDesZKjeyqHFnhxLDtbUKcq2N8xXYERg,AQACAAE/turtles.jpeg

Updatable Subspace Key

- Automatically versioned SSK keys
- Automatic updating
- Date hints
- Built on SSKs

Example:

USK@ozMQYaCEXnlHQQggITYSIeNSxqdMknqjOIYyCdMKqJA,gJyID9FRxaM5zDqI3D8-wHACAusOYa5Aag3M4tSEt~g,AQACAAE/Index/375/

Keyword Signed Key

- Similar to SSK
- Keyword is a string that allows derivation of public and private keys
- Anybody can read or write
- Fast communication, interactive
- Riddles, verification

Example:

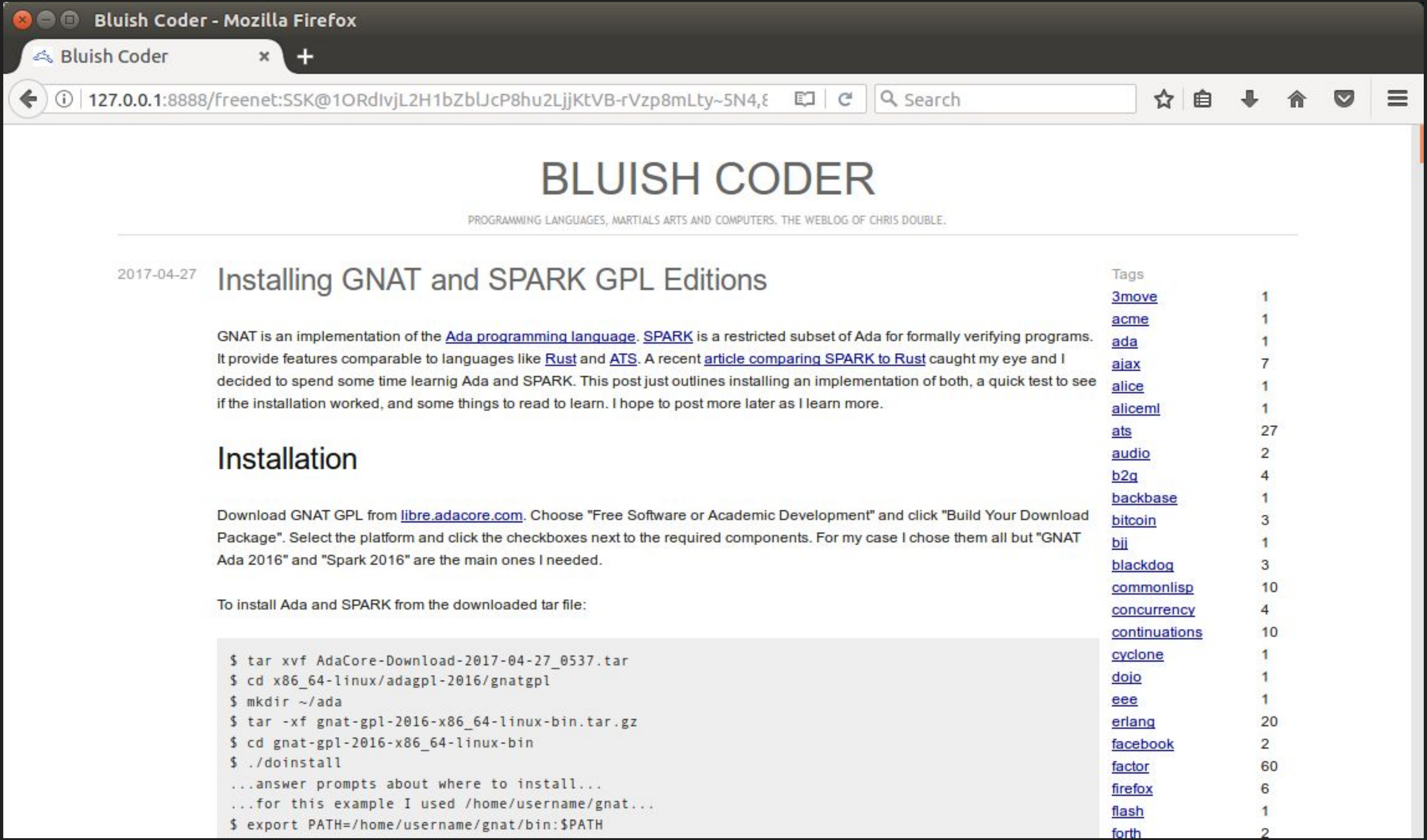
KSK@ArbitraryKeyName

Applications on Freenet

Applications

- Git
- Wikis
- Forums
- Chat
- Social Network
- Email
- More!

Freesites


Bluish Coder - Mozilla Firefox
Bluish Coder
127.0.0.1:8888/freenet:SSK@1ORdIvjL2H1bZbUcP8hu2LjjKtVB-rVzp8mLty~5N4,ε
Search

BLUISH CODER

PROGRAMMING LANGUAGES, MARTIALS ARTS AND COMPUTERS. THE WEBLOG OF CHRIS DOUBLE.

2017-04-27

Installing GNAT and SPARK GPL Editions

GNAT is an implementation of the Ada programming language. SPARK is a restricted subset of Ada for formally verifying programs. It provide features comparable to languages like Rust and ATS. A recent article comparing SPARK to Rust caught my eye and I decided to spend some time learnig Ada and SPARK. This post just outlines installing an implementation of both, a quick test to see if the installation worked, and some things to read to learn. I hope to post more later as I learn more.

Installation

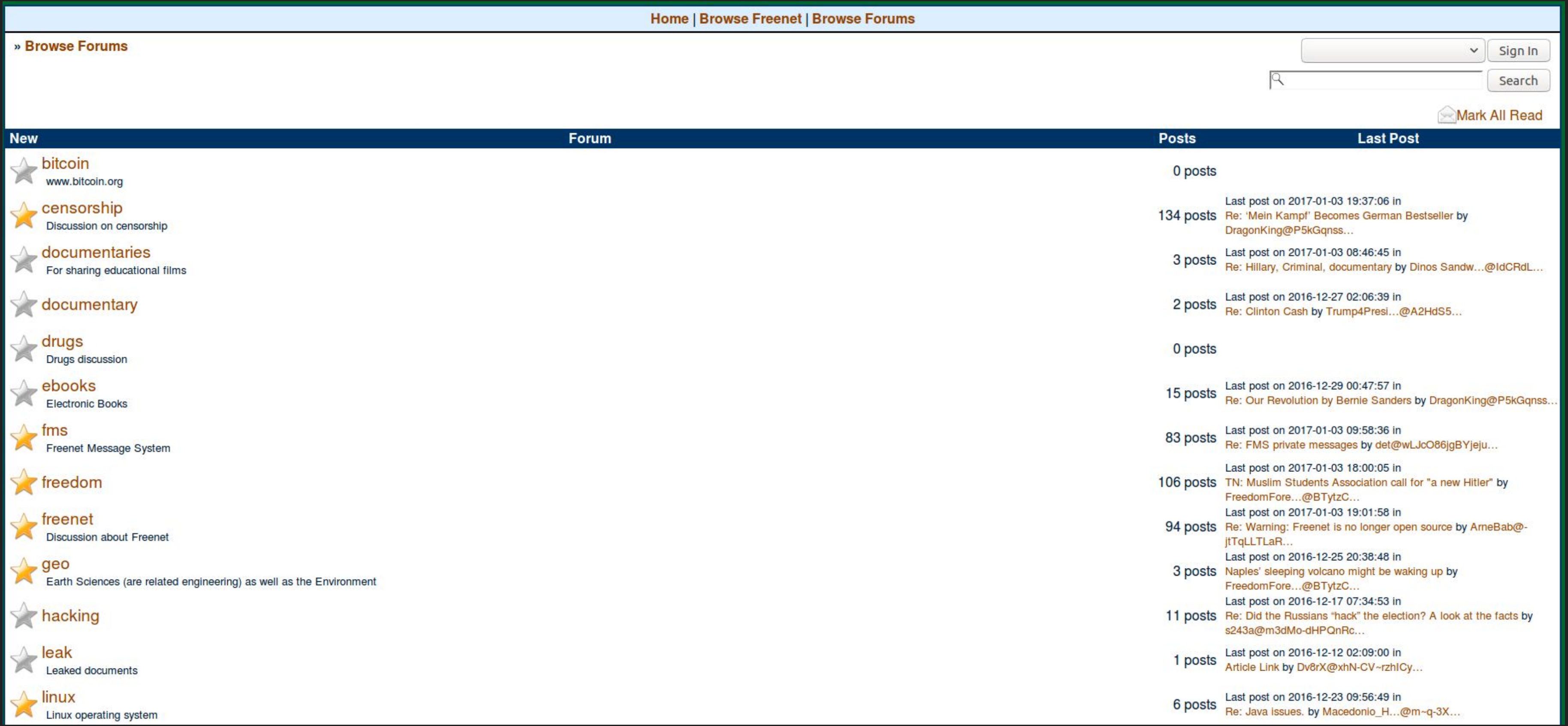
Download GNAT GPL from libre.adacore.com. Choose "Free Software or Academic Development" and click "Build Your Download Package". Select the platform and click the checkboxes next to the required components. For my case I chose them all but "GNAT Ada 2016" and "Spark 2016" are the main ones I needed.

To install Ada and SPARK from the downloaded tar file:

```
$ tar xvf AdaCore-Download-2017-04-27_0537.tar
$ cd x86_64-linux/adagpl-2016/gnatgpl
$ mkdir ~/ada
$ tar -xf gnat-gpl-2016-x86_64-linux-bin.tar.gz
$ cd gnat-gpl-2016-x86_64-linux-bin
$ ./doinstall
...answer prompts about where to install...
...for this example I used /home/username/gnat...
$ export PATH=/home/username/gnat/bin:$PATH
```

Tags	
3move	1
acme	1
ada	1
ajax	7
alice	1
aliceml	1
ats	27
audio	2
b2g	4
backbase	1
bitcoin	3
bij	1
blackdog	3
commonlisp	10
concurrency	4
continuations	10
cyclone	1
dojo	1
eee	1
erlang	20
facebook	2
factor	60
firefox	6
flash	1
forth	2

FMS

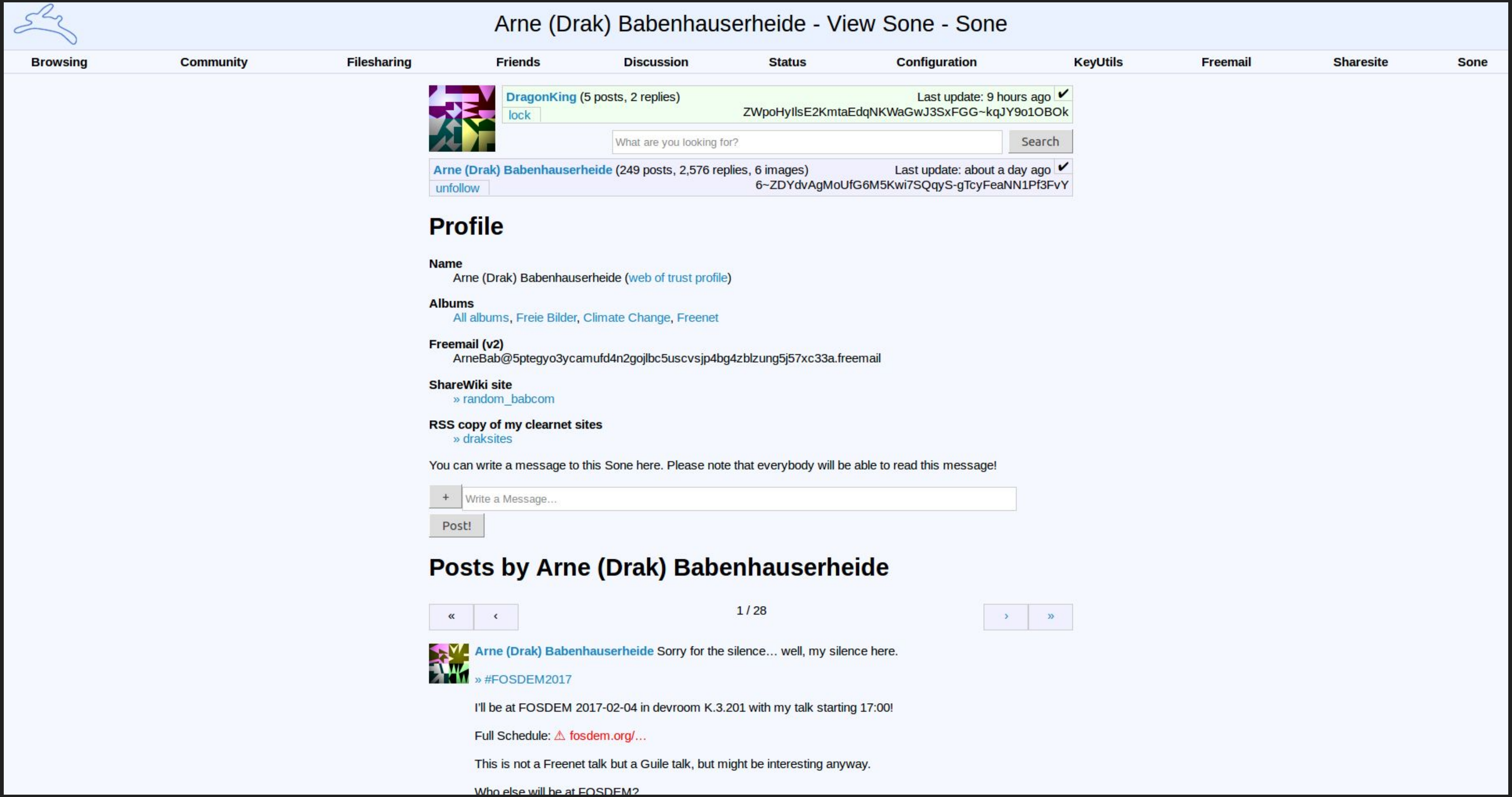


Home | Browse Freenet | Browse Forums

» Browse Forums

New	Forum	Posts	Last Post
☆	bitcoin www.bitcoin.org	0 posts	
★	censorship Discussion on censorship	134 posts	Last post on 2017-01-03 19:37:06 in Re: 'Mein Kampf' Becomes German Bestseller by DragonKing@P5kGqnss...
☆	documentaries For sharing educational films	3 posts	Last post on 2017-01-03 08:46:45 in Re: Hillary, Criminal, documentary by Dinos Sandw...@IdCRdL...
☆	documentary	2 posts	Last post on 2016-12-27 02:06:39 in Re: Clinton Cash by Trump4Presi...@A2HdS5...
☆	drugs Drugs discussion	0 posts	
☆	ebooks Electronic Books	15 posts	Last post on 2016-12-29 00:47:57 in Re: Our Revolution by Bernie Sanders by DragonKing@P5kGqnss...
★	fms Freenet Message System	83 posts	Last post on 2017-01-03 09:58:36 in Re: FMS private messages by det@wLJcO86jgBYjeju...
★	freedom	106 posts	Last post on 2017-01-03 18:00:05 in TN: Muslim Students Association call for "a new Hitler" by FreedomFore...@BTytzC...
★	freenet Discussion about Freenet	94 posts	Last post on 2017-01-03 19:01:58 in Re: Warning: Freenet is no longer open source by ArneBab@-jtTqLLTLaR...
★	geo Earth Sciences (are related engineering) as well as the Environment	3 posts	Last post on 2016-12-25 20:38:48 in Naples' sleeping volcano might be waking up by FreedomFore...@BTytzC...
☆	hacking	11 posts	Last post on 2016-12-17 07:34:53 in Re: Did the Russians "hack" the election? A look at the facts by s243a@m3dMo-dHPQnRc...
☆	leak Leaked documents	1 posts	Last post on 2016-12-12 02:09:00 in Article Link by Dv8rX@xhN-CV~rzhICy...
★	linux Linux operating system	6 posts	Last post on 2016-12-23 09:56:49 in Re: Java issues. by Macedonio_H...@m~q-3X...

Sone



Arne (Drak) Babenhauserheide - View Sone - Sone

DragonKing (5 posts, 2 replies) Last update: 9 hours ago
ZWpoHyIlsE2KmtaEdqNKWaGwJ3SxFGG~kqJY9o1OBOk

Arne (Drak) Babenhauserheide (249 posts, 2,576 replies, 6 images) Last update: about a day ago
6~ZDYdvAgMoUfG6M5Kwi7SQqyS-gTcyFeaNN1Pf3FvY

Profile

Name
Arne (Drak) Babenhauserheide (web of trust profile)

Albums
All albums, Freie Bilder, Climate Change, Freenet

Freemail (v2)
ArneBab@5ptegyo3ycamufd4n2gojlbc5uscvsjp4bg4zblzung5j57xc33a.freemail

ShareWiki site
» random_babcom

RSS copy of my clearnet sites
» draksites

You can write a message to this Sone here. Please note that everybody will be able to read this message!

Posts by Arne (Drak) Babenhauserheide

1 / 28

Arne (Drak) Babenhauserheide Sorry for the silence… well, my silence here.

» #FOSDEM2017

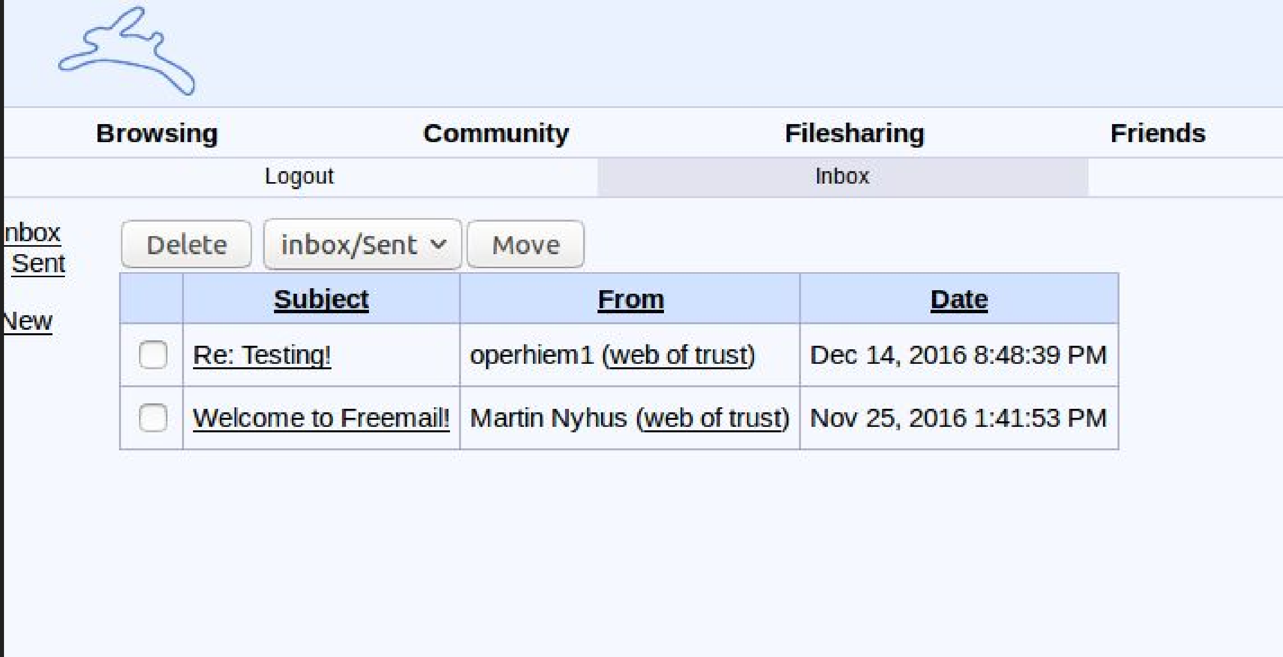
I'll be at FOSDEM 2017-02-04 in devroom K.3.201 with my talk starting 17:00!

Full Schedule: ⚠ fosdem.org/…

This is not a Freenet talk but a Guile talk, but might be interesting anyway.

Who else will be at FOSDEM?

Freemail



	Subject	From	Date
☐	Re: Testing!	operhiem1 (web of trust)	Dec 14, 2016 8:48:39 PM
☐	Welcome to Freemail!	Martin Nyhus (web of trust)	Nov 25, 2016 1:41:53 PM

Application Design

Thinking about your problem

- Plugin or Standalone?
- What kind of communication is necessary?
    - One to One
    - One to Many
    - Many to Many
- Cryptography is your friend
- Web of Trust

Example Scripts

Insert a file

```
import fcp

node = fcp.node.FCPNode()

node.put(file=filepath)

node.put(data=”this is a test”)

node.shutdown()
```

Get a file

```
import fcp

node = fcp.node.FCPNode()

data = node.get(uri=key)[1]

node.shutdown()
```

Insert files under an SSK

```
import fcp

n = fcp.node.FCPNode()

public, private = n.genkey()

filename = “test”

n.put(uri=private + filename, data=”hello, world!”)
```

KSK Example

```
import fcp

n = fcp.node.FCPNode()

key = “KSK@keyname”

n.put(uri=key, data=”Hello, world!”)
```

Demo Example

- Problem: Want to share large number of malware samples with community
- Solution: Create service that periodically shares samples
  - Allow users to grab latest
  - Allow users to see all files inserted
- Anonymity maintained

Demo Script

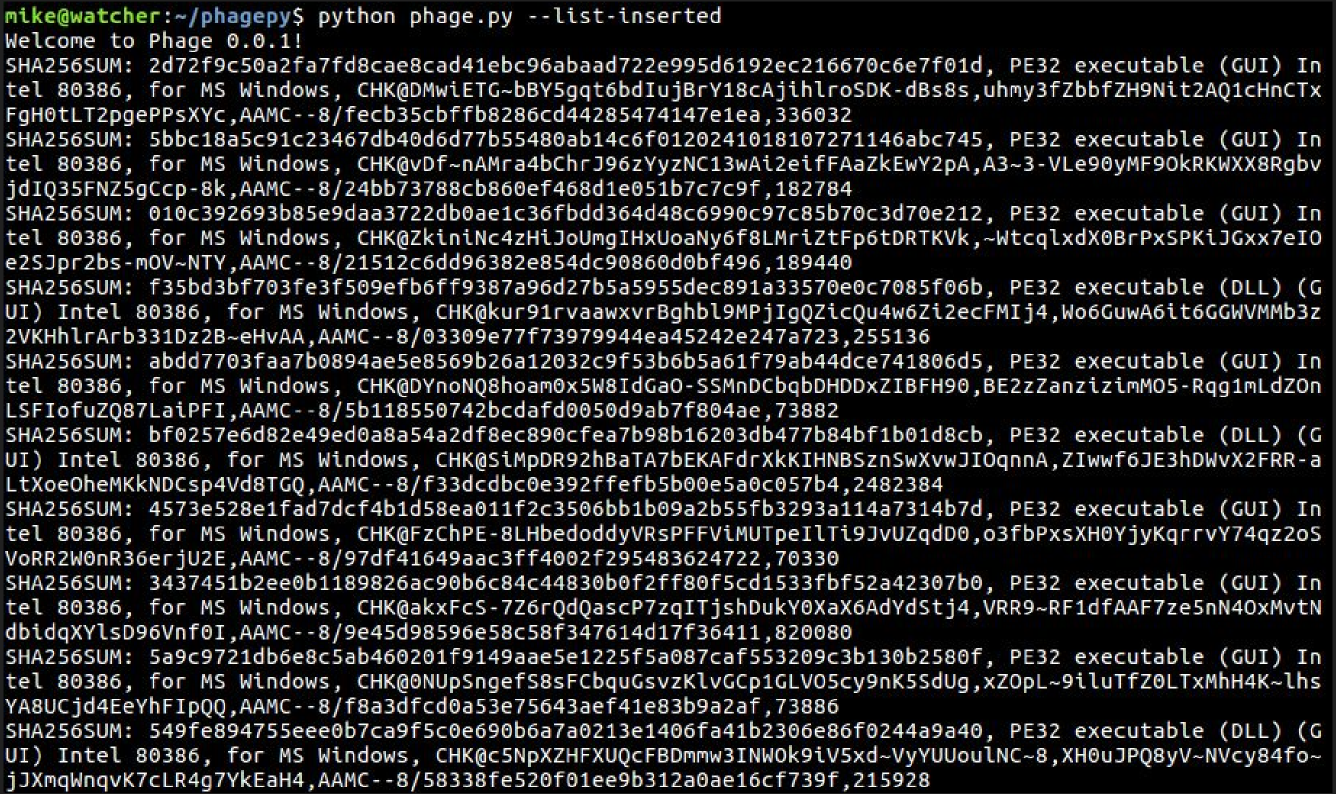
https://github.com/mgrube/phagepy

phage.py:

- Subscribe to a feed of virus/malware samples
- Request specific samples
- Update from anywhere
- Anonymous

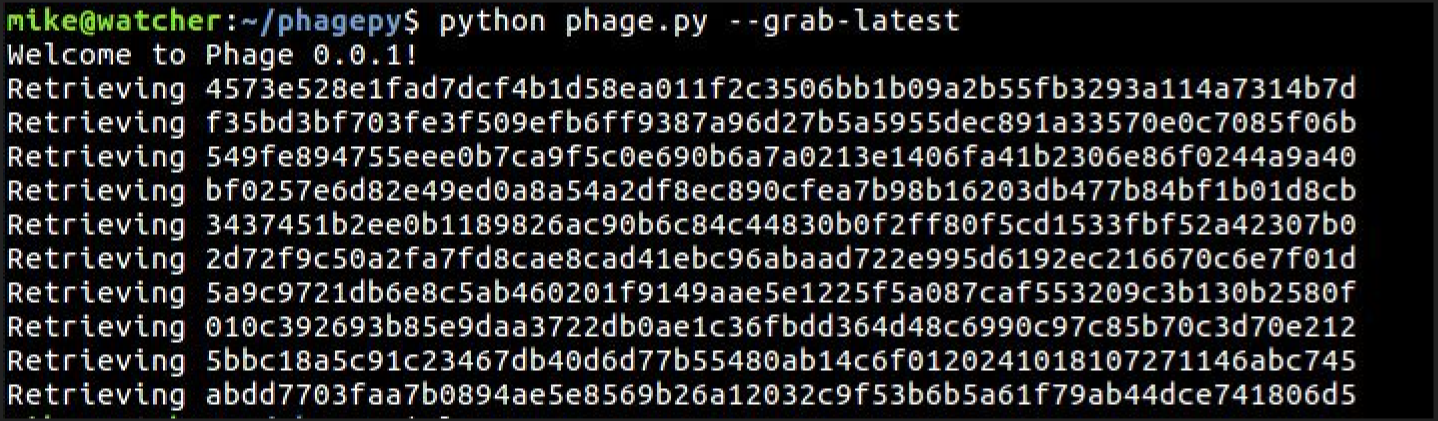
Questions?

All files inserted



```
mike@watcher:~/phagepy$ python phage.py --list-inserted
Welcome to Phage 0.0.1!
SHA256SUM: 2d72f9c50a2fa7fd8cae8cad41ebc96abaad722e995d6192ec216670c6e7f01d, PE32 executable (GUI) In
tel 80386, for MS Windows, CHK@DMwiETG~bBY5gqt6bdIujBrY18cAjihlroSDK-dBs8s,uhmy3fZbbfZH9Nit2AQ1cHnCTx
FgH0tLT2pgePPsXYc,AAMC--8/fecb35cbffb8286cd44285474147e1ea,336032
SHA256SUM: 5bbc18a5c91c23467db40d6d77b55480ab14c6f012024101810727 1146abc745, PE32 executable (GUI) In
tel 80386, for MS Windows, CHK@vDf~nAMra4bChrJ96zYyzNC13wAi2eifFAaZkEwY2pA,A3~3-VLe90yMF9OkRKWXX8Rgbv
jdIQ35FNZ5gCcp-8k,AAMC--8/24bb73788cb860ef468d1e051b7c7c9f,182784
SHA256SUM: 010c392693b85e9daa3722db0ae1c36fbdd364d48c6990c97c85b70c3d70e212, PE32 executable (GUI) In
tel 80386, for MS Windows, CHK@ZkiniNc4zHiJoUmgIHxUoaNy6f8LMriZtFp6tDRTKVk,~WtcqlxdX0BrPxSPKiJGxx7eIO
e2SJpr2bs-mOV~NTY,AAMC--8/21512c6dd96382e854dc90860d0bf496,189440
SHA256SUM: f35bd3bf703fe3f509efb6ff9387a96d27b5a5955dec891a33570e0c7085f06b, PE32 executable (DLL) (G
UI) Intel 80386, for MS Windows, CHK@kur91rvaawxvrBghbl9MPjIgQZicQu4w6Zi2ecFMIj4,Wo6GuwA6it6GGWVMMb3z
2VKHhlrArb331Dz2B~eHvAA,AAMC--8/03309e77f73979944ea45242e247a723,255136
SHA256SUM: abdd7703faa7b0894ae5e8569b26a12032c9f53b6b5a61f79ab44dce741806d5, PE32 executable (GUI) In
tel 80386, for MS Windows, CHK@DYnoNQ8hoam0x5W8IdGaO-SSMnDCbqbDHDDxZIBFH90,BE2zZanzizimMO5-Rqg1mLdZOn
LSFIofuZQ87LaiPFI,AAMC--8/5b118550742bcdafd0050d9ab7f804ae,73882
SHA256SUM: bf0257e6d82e49ed0a8a54a2df8ec890cfea7b98b16203db477b84bf1b01d8cb, PE32 executable (DLL) (G
UI) Intel 80386, for MS Windows, CHK@SiMpDR92hBaTA7bEKAFdrXkKIHNBSznSwXvwJIOqnnA,ZIwwf6JE3hDWvX2FRR-a
LtXoeOheMKkNDCsp4Vd8TGQ,AAMC--8/f33dcdbc0e392ffefb5b00e5a0c057b4,2482384
SHA256SUM: 4573e528e1fad7dcf4b1d58ea011f2c3506bb1b09a2b55fb3293a114a7314b7d, PE32 executable (GUI) In
tel 80386, for MS Windows, CHK@FzChPE-8LHbedoddyVRsPFFViMUTpeIlTi9JvUZqdD0,o3fbPxsXH0YjyKqrrvY74qz2oS
VoRR2W0nR36erjU2E,AAMC--8/97df41649aac3ff4002f295483624722,70330
SHA256SUM: 3437451b2ee0b1189826ac90b6c84c44830b0f2ff80f5cd1533fbf52a42307b0, PE32 executable (GUI) In
tel 80386, for MS Windows, CHK@akxFcS-7Z6rQdQascP7zqITjshDukY0XaX6AdYdStj4,VRR9~RF1dfAAF7ze5nN4OxMvtN
dbidqXYlsD96Vnf0I,AAMC--8/9e45d98596e58c58f347614d17f36411,820080
SHA256SUM: 5a9c9721db6e8c5ab460201f9149aae5e1225f5a087caf553209c3b130b2580f, PE32 executable (GUI) In
tel 80386, for MS Windows, CHK@0NUpSngefS8sFCbquGsvzKlvGCp1GLVO5cy9nK5SdUg,xZOpL~9iluTfZ0LTxMhH4K~lhs
YA8UCjd4EeYhFIpQQ,AAMC--8/f8a3dfcd0a53e75643aef41e83b9a2af,73886
SHA256SUM: 549fe894755eee0b7ca9f5c0e690b6a7a0213e1406fa41b2306e86f0244a9a40, PE32 executable (DLL) (G
UI) Intel 80386, for MS Windows, CHK@c5NpXZHFXUQcFBDmmw3INWOk9iV5xd~VyYUUoulNC~8,XH0uJPQ8yV~NVcy84fo~
jJXmqWnqvK7cLR4g7YkEaH4,AAMC--8/58338fe520f01ee9b312a0ae16cf739f,215928
```

Grab most recently inserted



```
mike@watcher:~/phagepy$ python phage.py --grab-latest
Welcome to Phage 0.0.1!
Retrieving 4573e528e1fad7dcf4b1d58ea011f2c3506bb1b09a2b55fb3293a114a7314b7d
Retrieving f35bd3bf703fe3f509efb6ff9387a96d27b5a5955dec891a33570e0c7085f06b
Retrieving 549fe894755eee0b7ca9f5c0e690b6a7a0213e1406fa41b2306e86f0244a9a40
Retrieving bf0257e6d82e49ed0a8a54a2df8ec890cfea7b98b16203db477b84bf1b01d8cb
Retrieving 3437451b2ee0b1189826ac90b6c84c44830b0f2ff80f5cd1533fbf52a42307b0
Retrieving 2d72f9c50a2fa7fd8cae8cad41ebc96abaad722e995d6192ec216670c6e7f01d
Retrieving 5a9c9721db6e8c5ab460201f9149aae5e1225f5a087caf553209c3b130b2580f
Retrieving 010c392693b85e9daa3722db0ae1c36fbdd364d48c6990c97c85b70c3d70e212
Retrieving 5bbc18a5c91c23467db40d6d77b55480ab14c6f01202410181072711146abc745
Retrieving abdd7703faa7b0894ae5e8569b26a12032c9f53b6b5a61f79ab44dce741806d5
```